-- STRUCTURE OF DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEM --.

In the Specification:

Please delete the section entitled "Cross-Reference to Related Application" on page 1 and insert therefor:

--CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation of U.S. Patent Application No. 09/290,363, filed April 12, 1999 and entitled "ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT", and claims the benefit of U.S. Provisional Application No. 60/126,614, filed March 27, 1998 and entitled "ENFORCEMENT ARCHITECTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT", both of which are hereby incorporated by reference.--

In the Claims:

Please cancel claims 1-105 without prejudice.

Please insert new claims 106-163, as follows:

106. A digital rights management (DRM) system operating on a computing device when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner, the system comprising:

a license store for storing one or more digital licenses on the computing device;

a license evaluator for determining whether any licenses stored in the license store correspond to the requested digital content, for determining whether any such corresponding licenses are valid, for reviewing license rules in each such valid license, and for determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought; and

a state store for maintaining state information corresponding to each license in the license store, the state information being created and updated by the license evaluator as necessary.

107. The DRM system of claim 106 wherein the license evaluator is a trusted component thereof.

108. The DRM system of claim 107 wherein the license evaluator runs in a protected environment on the computing device such that the user is denied access to such license evaluator.

109. The DRM system of claim 106 wherein the license evaluator effectuates acquiring an enabling, valid license if no such enabling, valid license is located and if such enabling, valid license is available.

110. The DRM system of claim 109 wherein the license evaluator refers to license acquisition information attached to the digital content during effectuating acquiring an enabling, valid license, the license acquisition information including data selected from a group consisting of types of licenses available and a network site at which a license server may be accessed.

111. The DRM system of claim 110 wherein the license evaluator exchanges information with the license server during acquisition of an enabling, valid license.

112. The DRM system of claim 110 further comprising a black box for performing encryption and decryption functions as part of the evaluation of any license, the black box having a first unique public / private key pair (PU-BB1, PR-BB1) that is employed as part of the evaluation of any license, wherein the license server refuses to issue a license to the license evaluator if the black box is not current.

113. The DRM system of claim 112 wherein the license evaluator requests a current black box from a black box server, receives the requested black box, and installs the received black box on the computing device, the received black box having a second unique public / private key pair (PU-BB2, PR-BB2) different from the first unique public / private key pair (PU-BB1, PR-BB1).

114. The DRM system of claim 110 wherein the license evaluator receives an enabling, valid license from the license server and stores the received license in the license store.

115. The DRM system of claim 106 wherein in determining whether the license enables the requesting user to render the requested digital content in the manner sought, the license evaluator has access to data on the computing device, such data being selected from a group consisting of:

an identification of the computing device and/or particular aspects thereof;

an identification of the user and/or particular aspects thereof;

an identification of an application to be employed to render the digital content and/or particular aspects thereof;

a system clock; and

combinations thereof.

116. The DRM system of claim 106 further comprising a black box for performing encryption and decryption functions as part of the evaluation of any license.

117. The DRM system of claim 116 wherein the black box is a trusted component thereof.

118. The DRM system of claim 117 wherein the black box runs in a protected environment on the computing device such that the user is denied access to such black box.

119. The DRM system of claim 116 wherein the black box works in conjunction with the license evaluator to decrypt / encrypt information as part of the evaluation of any license.

120. The DRM system of claim 116 wherein the license evaluator selects an enabling, valid license and works with the black box to obtain a decryption key (KD) from the selected license, and wherein the black box employs such decryption key (KD) to decrypt the protected digital content.

121. The DRM system of claim 116 wherein the black box decrypts the protected digital content when the license evaluator determines that a license in fact enables the requesting user to render the requested digital content in the manner sought.

122. The DRM system of claim 121 wherein the black box works in conjunction with the license evaluator to decrypt / encrypt information as part of the evaluation of any license, and wherein the black box has a unique public / private key pair (PU-BB, PR-BB) that is employed as part of the evaluation of any license, and that is also employed to obtain a decryption key (KD) for decrypting the protected digital content.

123. The DRM system of claim 106 wherein the license store is at least a portion of a memory storage device on the computing device.

124. The DRM system of claim 123 wherein the license store is a directory of a memory drive.

125. The DRM system of claim 124 wherein the memory drive is selected from a group consisting of a soft disk drive, a hard disk drive, and a network drive.

126. The DRM system of claim 106 wherein the state store is a trusted component thereof.

127. The DRM system of claim 126 wherein the state store runs in a protected environment on the computing device such that the user is denied access to such state store.

128. The DRM system of claim 106 wherein each license in the license store may be removed therefrom, and wherein the state store also maintains state information corresponding to each license formerly in the license store.

129. A computing device having a digital rights management (DRM) system operating thereon when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner, the DRM system comprising:

a license store for storing one or more digital licenses on the computing device;

a license evaluator for determining whether any licenses stored in the license store correspond to the requested digital content, for determining whether any such corresponding licenses are valid, for reviewing license rules in each such valid license, and for determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought; and

a state store for maintaining state information corresponding to each license in the license store, the state information being created and updated by the license evaluator as necessary.

130. The computing device of claim 129 wherein the license evaluator is a trusted component of the DRM system.

131. The computing device of claim 130 wherein the license evaluator runs in a protected environment thereon such that the user is denied access to such license evaluator.

132. The computing device of claim 129 wherein the license evaluator effectuates acquiring an enabling, valid license if no such enabling, valid license is located and if such enabling, valid license is available.

133. The computing device of claim 132 wherein the license evaluator refers to license acquisition information attached to the digital content during effectuating acquiring an enabling, valid license, the license acquisition information including data selected from a group consisting of types of licenses available and a network site at which a license server may be accessed.

134. The computing device of claim 133 wherein the license evaluator exchanges information with the license server during acquisition of an enabling, valid license.

135. The computing device of claim 133 wherein the DRM system further comprises a black box for performing encryption and decryption functions as part of the evaluation of any license, the black box having a first unique public / private key pair (PU-BB1, PR-BB1) that is employed as part of the evaluation of any license, wherein the license server refuses to issue a license to the license evaluator if the black box is not current.

136. The computing device of claim 135 wherein the license evaluator requests a current black box from a black box server, receives the requested black box, and installs the

received black box on the computing device, the received black box having a second unique public / private key pair (PU-BB2, PR-BB2) different from the first unique public / private key pair (PU-BB1, PR-BB1).

137. The computing device of claim 133 wherein the license evaluator receives an enabling, valid license from the license server and stores the received license in the license store.

138. The computing device of claim 129 wherein in determining whether the license enables the requesting user to render the requested digital content in the manner sought, the license evaluator has access to data on the computing device, such data being selected from a group consisting of:

an identification of the computing device and/or particular aspects thereof;

an identification of the user and/or particular aspects thereof;

an identification of an application to be employed to render the digital content and/or particular aspects thereof;

a system clock; and

combinations thereof.

139. The computing device of claim 129 wherein the DRM system further comprises a black box for performing encryption and decryption functions as part of the evaluation of any license.

140. The computing device of claim 139 wherein the black box is a trusted component of the DRM system.

141. The computing device of claim 140 wherein the black box runs in a protected environment thereon such that the user is denied access to such black box.

142. The computing device of claim 139 wherein the black box works in conjunction with the license evaluator to decrypt / encrypt information as part of the evaluation of any license.

143. The computing device of claim 139 wherein the license evaluator selects an enabling, valid license and works with the black box to obtain a decryption key (KD) from the selected license, and wherein the black box employs such decryption key (KD) to decrypt the protected digital content.

144. The computing device of claim 139 wherein the black box decrypts the protected digital content when the license evaluator determines that a license in fact enables the requesting user to render the requested digital content in the manner sought.

145. The computing device of claim 144 wherein the black box works in conjunction with the license evaluator to decrypt / encrypt information as part of the evaluation of any license, and wherein the black box has a unique public / private key pair (PU-BB, PR-BB) that is employed as part of the evaluation of any license, and that is also employed to obtain a decryption key (KD) for decrypting the protected digital content.

146. The computing device of claim 129 wherein the license store is at least a portion of a memory storage device on the computing device.

147. The computing device of claim 146 wherein the license store is a directory of a memory drive.

148. The computing device of claim 147 wherein the memory drive is selected from a group consisting of a soft disk drive, a hard disk drive, and a network drive.

149. The computing device of claim 129 wherein the state store is a trusted component of the DRM system.

150. The computing device of claim 149 wherein the state store runs in a protected environment thereon such that the user is denied access to such state store.

151. The computing device of claim 129 wherein each license in the license store may be removed therefrom, and wherein the state store also maintains state information corresponding to each license formerly in the license store.

152. A computer-readable medium having computer-executable instructions stored thereon for operating a digital rights management (DRM) system on a computing device when a user requests that a protected piece of digital content be rendered by the computer device in a particular manner, the instructions performing a method comprising:

storing one or more digital licenses in a license store on the computing device;

determining whether any licenses stored in the license store correspond to the requested digital content;

determining whether any such corresponding licenses are valid;

reviewing license rules in each such valid license;

determining based on such reviewed license rules whether such license enables the requesting user to render the requested digital content in the manner sought; and

maintaining in a state store on the computing device state information corresponding to each license in the license store, the state information being created and updated as necessary.

153. The method of claim 152 further comprising acquiring an enabling, valid license if no such enabling, valid license is located and if such enabling, valid license is available.

154. The method of claim 153 further comprising referring to license acquisition information attached to the digital content to effectuate acquiring an enabling, valid license, the license acquisition information including data selected from a group consisting of types of licenses available and a network site at which a license server may be accessed.

155. The method of claim 154 further comprising exchanging information with the license server during acquisition of an enabling, valid license.

156. The method of claim 154 further comprising performing encryption and decryption functions as part of the evaluation of any license with a black box having a first unique public / private key pair (PU-BB1, PR-BB1) that is employed as part of the evaluation of any license.

157. The method of claim 156 wherein the license server refuses to issue a license to the license evaluator if the black box is not current, and wherein the method comprises:

requesting a current black box from a black box server;

receiving the requested black box; and

installing the received black box on the computing device, the received black box having a second unique public / private key pair (PU-BB2, PR-BB2) different from the first unique public / private key pair (PU-BB1, PR-BB1).

158. The method of claim 152 wherein determining whether the license enables the requesting user to render the requested digital content in the manner sought comprises determining whether the license enables the requesting user to render the requested digital content in the manner sought based on data stored on the computing device, such data being selected from a group consisting of:

an identification of the computing device and/or particular aspects thereof;

an identification of the user and/or particular aspects thereof;

an identification of an application to be employed to render the digital content and/or particular aspects thereof;

a system clock; and

combinations thereof.

159. The method of claim 152 further comprising performing encryption and decryption functions as part of the evaluation of any license.

160. The method of claim 159 comprising selecting an enabling, valid license, obtaining a decryption key (KD) from the selected license, and employing such decryption key (KD) to decrypt the protected digital content.

161. The method of claim 159 comprising decrypting the protected digital content upon determining that a license in fact enables the requesting user to render the requested digital content in the manner sought.

162. The method of claim 159 further comprising performing encryption and decryption functions as part of the evaluation of any license with a black box having a unique public / private key pair (PU-BB, PR-BB) that is employed as part of the evaluation of any license.

163. The method of claim 152 wherein each license in the license store may be removed therefrom, the method further comprising maintaining state information in the state store corresponding to each license formerly in the license store.

In the Abstract: